(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11239169 A**

(43) Date of publication of application: **31.08.99**

(51) Int. Cl **H04L 12/54**
H04L 12/58
G06F 13/00

(21) Application number: **10041446**

(22) Date of filing: **24.02.98**

(71) Applicant: **SUMITOMO ELECTRIC IND LTD**

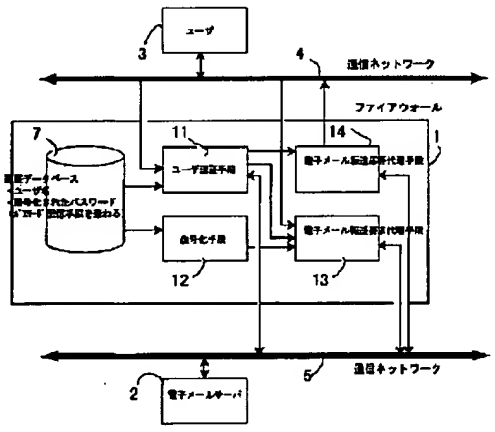
(72) Inventor: **KOREKAWA NORIO**
NAKAMORI KOSHU
MAEYAMA YOSHIKUNI

(54) **FIREWALL DEVICE COPING WITH ELECTRONIC MAIL**

(57) Abstract:

PROBLEM TO BE SOLVED: To safely utilize an electronic mail server of an internal communications channel from an external communications channel by requesting electronic mail to the electronic mail server corresponding to a request from a user by an electronic mail transfer request representing means after a prescribed procedure and transmitting a response from the electronic mail server to the user.

SOLUTION: Relating to a firewall, after the user 3 connected to a communications network 4 is authenticated by a user authentication means 11, the electronic mail is requested to the electronic mail server 2 corresponding to the request of the user 3 instead of the user 3 by the electronic mail transfer request representing means 13 and the response from the electronic mail server 2 is transmitted to the user 3 by an electronic mail transfer response representing means 14. Since authentication by the user authentication means 11 is performed by a disposable password, even when an intruder eavesdrops the disposable password, authentication can not be performed by using it.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－239169

(43)公開日　平成11年(1999)８月31日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	12/54		Ｈ０４Ｌ	11/20	１０１Ｂ
	12/58		Ｇ０６Ｆ	13/00	３５１Ｚ
Ｇ０６Ｆ	13/00	３５１			

審査請求　未請求　請求項の数４　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－41446

(22)出願日　平成10年(1998)２月24日

(71)出願人　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番33号

(72)発明者　是川　則雄
大阪府大阪市此花区島屋一丁目１番３号
住友電気工業株式会社大阪製作所内

(72)発明者　中森　弘修
大阪府大阪市此花区島屋一丁目１番３号
住友電気工業株式会社大阪製作所内

(72)発明者　前山　欣邦
大阪府大阪市此花区島屋一丁目１番３号
住友電気工業株式会社大阪製作所内

(74)代理人　弁理士　上代　哲司　（外２名）

(54)【発明の名称】　電子メール対応ファイアウォール装置

(57)【要約】

【課題】　従来、外部のネットワーク上のパソコンなどから、ファイアウォールで守られたネットワーク上のメールサーバへ接続するには、機密保護の観点から、容易なことではなかった。

【解決手段】　本発明では、ユーザ認証手段、電子メール転送要求代理手段、および電子メール転送応答代理手段を備えたファイアウォールと電子メールサーバを組み合わせることにより、維持管理が容易で、比較的安価で、かつ、高度な機密性を有するメールシステムを備えた、ファイアウォール装置を構築できる。

1

【特許請求の範囲】

【請求項１】　複数の通信ネットワークに接続されており、その内のある通信ネットワーク（４）からの通信を選択的に別の通信ネットワーク（５）に伝送するファイアウォール装置において、

通信ネットワーク（４）に接続されているユーザ（３）を、使い捨てパスワードを用いて認証するユーザ認証手段（１１）と、ユーザ（３）の電子メールの要求に応じて通信ネットワーク（５）に接続されている電子メールサーバ（２）に対して電子メールに関する要求を代行する電子メール転送要求代理手段（１３）と、

電子メールサーバ（２）からの応答をユーザ（３）に送信する電子メール転送応答代理手段（１４）とを有し、

通信ネットワーク（４）に接続されているユーザ（３）の認証を行なった後に、そのユーザ（３）の代わりにユーザ（３）からの要求に応じて電子メールサーバ（２）に電子メールの要求を行い、電子メールサーバ（２）からの応答をユーザ（３）に送信することを特徴とする電子メール対応ファイアウォール装置。

【請求項２】複数の通信ネットワークに接続されており、その内のある通信ネットワーク（４）からの通信を選択的に別の通信ネットワーク（５）に伝送するファイアウォール装置において、

通信ネットワーク（４）に接続されているユーザ（３）から使い捨てパスワードを受け取り、この使い捨てパスワードを通信ネットワーク（５）に接続されている認証サーバ（８）に送信してユーザ認証の可否を問い合せるユーザ認証問合手段（１５）と、

ユーザ（３）の電子メールの要求に応じて通信ネットワーク（５）に接続されている電子メールサーバ（２）に対して電子メールに関する要求を代行する電子メール転送要求代理手段（１３）と、

電子メールサーバ（２）からの応答をユーザ（３）に送信する電子メール転送応答代理手段（１４）とを有し、

通信ネットワーク（４）に接続されているユーザ（３）が認証サーバ（８）によって認証された後に、そのユーザ（３）の代わりにユーザ（３）からの要求に応じて電子メールサーバ（２）に電子メールの要求を行い、電子メールサーバ（２）からの応答をユーザ（３）に送信することを特徴とする電子メール対応ファイアウォール装置。

【請求項３】請求項１または請求項２に記載の電子メール対応ファイアウォール装置において、さらに、

ユーザ（３）の電子メールサーバ（２）に対するパスワードＲを記憶するパスワード記憶手段、または、パスワードＲを通信ネットワーク（５）に接続されているパスワード記憶装置から取得するパスワード取得手段（１６）を有し、

通信ネットワーク（４）に接続されているユーザ（３）の認証を行なった後は、パスワード記憶手段またはパスワード取得手段（１６）から得たパスワードＲを使って電子メールサーバ（２）に対する電子メールの要求を行なうことを特徴とする電子メール対応ファイアウォール装置。

2

【請求項４】請求項３に記載の電子メール対応ファイアウォール装置において、さらに、暗号化されたパスワードＶを平文のパスワードＷに戻す復号化手段を有し、

パスワード記憶手段またはパスワード取得手段から得たパスワードＶを平文のパスワードＷに戻したのちに、その平文のパスワードＷを使って電子メールサーバ（２）に対する電子メールの要求を行なうことを特徴とする電子メール対応ファイアウォール装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不特定の第三者にも利用される通信チャンネル（以下、外部通信チャンネル）と特定の関係者しか利用されない（不特定の第三者には利用されない）通信チャンネル（以下、内部通信チャンネル）の間に設けるファイアウォール装置（以下、ファイアウォールと略称する）に関するものである。特に、内部通信チャンネルに接続されている電子メールサーバに、外部通信チャンネルからアクセスを安全に行ないたい場合に用いると好適である。

【０００２】

【従来の技術】電子メールは、インターネットの拡大と共に普及が進んでおり、一企業内での従業員相互間の連絡にもしばしば使われるようになってきている。インターネット関連で市販されているツールを、企業内のみの情報伝達に流用することも広く行なわれており、イントラネットと呼ばれている。イントラネットを使って、電子メールを従業員相互間でやりとりする場合の構成を図３に示す。図３において、２２はイントラネットを構成する通信チャンネルである。図３では、便宜上リング状に書いてあるが、通信チャンネルを構成する通信機器をすべてリング状に接続する必要はなく、ツリー状、スター状等、各種のトポロジで接続することができる。２１は電子メールサーバである。電子メールを使用したい従業員等、すなわち、ユーザは、自分の操作するコンピュータ（以下、ユーザ用コンピュータ）を使って、電子メールサーバにアクセスする。具体的には、各ユーザがユーザ用コンピュータ２３、２４、…を使って送信した電子メールは、一旦電子メールサーバ２１に蓄えられ、必要に応じて、取り出される。電子メールを電子メールサーバ２１から取り出す際は、ユーザ名、パスワードを電子メールサーバに与えることで、正当な利用者であることを示す。すなわち、ユーザ名とパスワードの組合せによって、ユーザの認証が行なわれる。２２は、企業内（所定の敷地や、建物）に設置されている。不正な第三者（以下、侵入者）が２２に流れている情報を不正に入手しようと思っても、その企業内に立ち入ることができ

ないため、２２に接続することができない。すなわち、企業内への立ち入りを制限することによって、物理的に２２は安全が保たれている。かかる場合は、電子メールのやりとりにおいても、さしたる機密保護のための処置は必要がない。機密保護のための処理が不要なので、各ユーザは、パスワードや電子メールを暗号化する手間を省くことができ、簡便かつ能率よく、電子メールを利用することができる。そのため、２２に流れるパスワードは、暗号化されていない平文のままである。

【０００３】次に、イントラネット２２を外部通信チャンネルに接続する場合の構成を図４に示す。外部通信チャンネルは、例えば、公衆回線やインターネットであり、侵入者の盗聴や攻撃はありうる。従って、イントラネット２２の内容がそのまま外部通信チャンネル２８に流出したり、外部通信チャンネル２８の内容が勝手にイントラネット２２に流れこんだりしないように、ファイアウォール２０を設ける。ファイアウォール２０は、真に意図した通信のみをイントラネット２２と外部通信チャンネル２８の間で通過させ、それ以外の通信を遮断する働きを持つ。また、ファイアウォール２０は、外部の侵入者からの根気良い攻撃に耐える必要がある。イントラネットの外のユーザに対し、電子メールサーバ２１の内容に、ファイアウォール２０を経て接続できないようにしてしまうと不便であるので、予め決められた種類の通信（例えば、電子メールの要求のみ）を、外部通信チャンネル２８からイントラネット２２へ通過させる設定が考えられる。安全さが多少は犠牲になるが、電子メールを外部ネットワークから読み出すことができるようになる。ただし、電子メールサーバ２１へのユーザ名とパスワードが平文のままでは、外部通信チャンネル２８を盗聴する侵入者によって簡単に悪用されてしまう。そこで、暗号化手続きを利用して、電子メールサーバ２１に対する認証を行なわなければならない。暗号化手続きによる認証としては、例えば、ＲＦＣ１９３９（ｆｔｐ：／／ｄｓ．ｉｎｔｅｒｎｉｃ．ｎｅｔ／ｒｆｃ／ｒｆｃ１９３９．ｔｘｔ）に規定されているＰＯＰ３（Ｐｏｓｔ Ｏｆｆｉｃｅ Ｐｒｏｔｏｃｏｌ－ｖｅｒｓｉｏｎ ３）のＡＰＯＰコマンドを使用することができる。この様にすれば、電子メールを外部ネットワークから読み出すことができるようになる（従来技術ａ）。また、ファイアウォールに対する安全性を高めるために、暗号化手続きによる認証をファイアウォールにも適用するという構成（以下、従来技術ｂ）も取り得る。すなわち、電子メールサーバへの電子メールの要求に先立って、まず、ファイアウォールに対して暗号化手続きによる認証を行なうという構成である。

【０００４】

【発明が解決しようとする課題】従来技術ａで説明したように、ＡＰＯＰコマンドを使えば、電子メールサーバへのパスワードの盗聴そのものに対する耐性は得られる。しかし、電子メールに関する要求はファイアウォールを通過するように設定されているので、安全さが多少犠牲になっている。たとえば、侵入者は外部ネットワークを盗聴していると、電子メールの要求の通信だけはファイアウォールを通過することを発見しうる。そして、侵入者が電子メールの要求の通信を外部ネットワークから流し込むと、その通信はファイアウォール２０を抜けてイントラネット２２に入ることになる。すると、電子メールサーバがその電子メールの要求を認証しなくても（無視しても）、電子メールの要求が大量に流れれば、イントラネット２２の伝送容量を上回った時点で、通信障害が発生する。このようにして、イントラネット２２を使った企業内活動を停止させる事態が生じうる。つまり、強い破壊の意図を持った侵入者に対しては防御ができない。これは、ＰＯＰ３のＡＰＯＰコマンドの規約そのものが、電子メールサーバのみを考慮において構築されたために内在することとなった、システム構築上の限界である。

【０００５】従来技術ｂでは、ファイアウォールに対する認証を済ませなければ、電子メールに関する通信も通過できないので、ファイアウォール越しの攻撃は防御できる。しかし、電子メールサーバへの電子メールの要求に先立って、まず、ファイアウォールに対して暗号化手続きによる認証を行なわければならない。すなわち、ファイアウォールへの認証手続きと、ＰＯＰ３への認証手続きを共に行なわねばならず、煩雑である。また、ユーザ登録の維持や認証手続きの管理の手間も二重に必要になり、管理コストの増大という欠点が新たに生じる。

【０００６】以上の様に、従来技術による外部ネットワークから内部ネットワークの電子メールの読み出しは、本質的に安全性に欠ける（従来技術ａ）か、煩雑な手続きや管理コストの増大（従来技術ｂ）という問題が避けられなかった。　なお、ＡＰＯＰコマンドはＰＯＰ３のオプションであり、これが電子メールサーバには実装されているとは限らない。イントラネットは、最初は簡便な方法で構築し、その後は管理者の熟達や利用者数の増大に応じて発展させるのが普通である。ＡＰＯＰコマンドのない簡便で入手しやすい電子メールサーバを使ってイントラネットを構築すると、そのままでは後に外部ネットワークに接続できないというのでは困る。仮に、ＡＰＯＰコマンドのある電子メールサーバに交換するとなると、交換の費用や手間等の出費が嵩んでしまう。また、そもそもＡＰＯＰコマンドを実装した電子メールサーバは実はあまり市販されていないので、現実には、上記に述べたシステムすら構築しにくいという欠点もある。本願発明は、これらの欠点を解消して、安全に外部通信チャンネルから内部通信チャンネルの電子メールサーバを利用する手段を提供するものである。

【０００７】

【課題を解決するための手段】図１に請求項１と３と４

を組み合わせたファイアウォールの構成を示す。４は外部通信チャンネルに相当する通信ネットワークであり、５は内部通信チャンネルに相当する通信ネットワークである。３は通信ネットワークに接続されているユーザである。言うまでもなく、通信ネットワーク４に接続されているのは、実際には、ユーザ３が操作する個人用コンピュータ（不図示）であり、ユーザ３はこの個人用コンピュータを介して通信ネットワーク４を使用する。ここでは、発明の本質を簡潔に表すために、途中に介在する個人用コンピュータを省いて、ユーザ３が通信ネットワークを使用するものとして説明する。２は通信ネットワーク４に接続されている電子メールサーバ２であり、通信ネットワーク５に接続されている他の装置やユーザからの要求に応じて、受信済みの電子メールを回答したり、電子メールを発信する処理を行なう。ユーザ３は電子メールサーバ２から、自己の電子メールを得たいと意図している。

【０００８】図２に請求項２と３と４を組み合わせたファイアウォールの構成を示す。８は通信ネットワーク５に接続された認証サーバであり、通信ネットワーク５に接続された他の装置からの要求に応じて、ユーザの認証を行なう。７は、認証サーバ８の有する認証データベースである。

【０００９】請求項１によるファイアウォールは、通信ネットワーク４に接続されているユーザ３を、使い捨てパスワードを用いて認証するユーザ認証手段１１と、ユーザ３の電子メールの要求に応じて５に接続されている電子メールサーバ２に対して電子メールに関する要求を代行する電子メール転送要求代理手段１３と、電子メールサーバ２からの応答をユーザ３に送信する電子メール転送応答代理手段１４と、を有することを特徴とする。なお、７は、ユーザ認証手段１１において必要となるユーザ名等の認証情報を記憶する認証データベースである。請求項２によるファイアウォールは、通信ネットワーク４に接続されているユーザ３から使い捨てパスワードを受け取り、この使い捨てパスワードを通信ネットワーク５に接続されている認証サーバ８に送信してユーザ認証の可否を問い合せるユーザ認証問い合せ手段１５と、ユーザ３の電子メールの要求に応じて通信ネットワーク５に接続されている電子メールサーバ２に対して電子メールに関する要求を代行する電子メール転送要求代理手段１３と、電子メールサーバ２からの応答をユーザ３に送信する電子メール転送応答代理手段１４と、を有することを特徴とする。請求項３によるファイアウォールは、請求項１又は２に加えてさらに、ユーザ３の電子メールサーバ２に対するパスワードＲを記憶するパスワード記憶手段、または、パスワードＲを通信ネットワーク５に接続されている認証データベース７（パスワード記憶装置）から取得するパスワード取得手段１６を有することを特徴とする。なお、パスワードはユーザの認証

に必要な情報と共に記憶することもできるので、図１と２では、認証データベースの中にパスワードも記憶されているものとして図示している。図２においては、認証データベース７の中のパスワードは、認証サーバ８を経由してパスワード取得手段１６に送られる。請求項４によるファイアウォール装置は、請求項１と３、又は、２と３に加えてさらに、暗号化されたパスワードＶを平文のパスワードＷに戻す復号化手段１２を有することを特徴とする。なお、図１と図２では、説明の便宜上、ファイアウォール１に接続する通信ネットワークが２つの場合を示したが、本発明は２つの通信チャンネルに限られることはなく、より多くの外部通信チャンネルや内部通信チャンネルを互いに接続する構成にすることも可能である。

【００１０】

【作用及び効果】請求項１によるファイアウォールは、ユーザ認証手段１１によって通信ネットワーク４に接続されているユーザ３の認証を行なった後に、電子メール転送要求代理手段１３によってそのユーザ３の代わりにユーザ３からの要求に応じて電子メールサーバ２に電子メールの要求を行い、電子メール転送応答代理手段１４によって電子メールサーバ２からの応答をユーザ３に送信する。ユーザ認証手段１１による認証は使い捨てパスワードにより行なわれるので、仮に侵入者がその使い捨てパスワードを盗聴したとしても、その使い捨てパスワードを使って侵入者が認証を行なうことができない。一方、電子メールサーバ２にとっては、ユーザ３からの電子メールの要求は通信ネットワーク５に接続されている電子メール転送要求代理手段１３から送られ、ユーザ３への電子メールに関する回答は通信ネットワーク５に接続されている電子メール転送応答代理手段１４に送るだけなので、これは通信ネットワーク５に接続されている他のユーザとのやりとりと変わらない。すなわち、請求項１の発明によれば、電子メールサーバを改変することなく、盗聴されても安全な方法による認証手続きを経た後に、外部通信チャンネルから電子メールサーバにアクセスできるようになる。そのため、

【００１１】　従来技術ａにおける、破壊の意図を持つ侵入者による電子メールの要求通信が外部通信チャンネルから内部通信チャンネルに無制限に流れ込む危険が、未然に回避できる。

【００１２】　従来技術ｂにおける、ファイアウォールと電子メールサーバの双方に対する認証手続きに比べ、認証の手間や管理の手間が減る。

【００１３】　電子メールサーバは、イントラネット用に既に導入したものがそのまま使える。そのため、新たな電子メールサーバを購入する費用や、使い方に熟達する手間が不要となる。また、電子メールサーバの交換する場合に生じる、イントラネット内部に対する電子メールのサービスの中断も避けられる。これらの点で、経済

的な利点が大きい。

【００１４】請求項２によるファイアウォールは、ユーザ認証問い合せ手段１５が通信ネットワーク５に接続されている認証サーバ８に依頼して、通信ネットワーク４に接続されているユーザ３を認証した後に、電子メール転送要求代理手段１３によってそのユーザ３の代わりにユーザ３からの要求に応じて電子メールサーバ２に電子メールの要求を行い、電子メール転送応答代理手段１４によって電子メールサーバ２からの応答をユーザ３に送信する。すなわち、請求項２の発明によれば、ファイアウォールとは別に用意した認証サーバに認証処理を行なわせることができる。そのため、請求項１の発明の効果に加えて、

【００１５】　ファイアウォールが外部からの攻撃に耐えられなくなって万一故障したとしても、認証サーバおよび認証サーバに蓄えている個々のユーザの認証データはそのまま残るので、より安全である。

【００１６】　複数の外部ネットワークを繋ぐためにファイアウォールを複数設けた場合など、認証結果が複数の場所で必要な場合、個々に認証データを記憶し、認証処理を行なわなくてすむ。つまり、個々のファイアウォールそれぞれに認証データを置いて認証処理を行なう場合に比べると記憶場所の削減や管理の一体化ができる。

【００１７】請求項３によるファイアウォールは、通信ネットワーク４に接続されているユーザ３の認証を行なった後は、認証データベース７（パスワード記憶手段）またはパスワード取得手段１６から得たパスワードＲを使って電子メールサーバ２に対する電子メールの要求を行なう。すなわち、請求項３の発明によれば、パスワードを外部通信チャンネルからではなく、ファイアウォールから又は、内部通信チャンネルから転送させることができる。そのため、請求項１または２の発明の効果に加えて、

【００１８】　ファイアウォールに対する認証とは別に、電子メールサーバの認証用のパスワードを、外部通信チャンネルにいるユーザが入力する手間を省ける。

【００１９】　パスワードを憶える手間を節約するため、ユーザが電子メールサーバに対してだけでなく当該ユーザが利用する複数の計算機に同一のものを使っている場合がある。外部通信チャンネルにいるユーザがパスワードを入力するとなると、覗き見等によりパスワードが漏洩し、別の計算機に悪用される可能性も生じる。本発明によれば、電子メールサーバ用のパスワードは当該企業の外に出る場合が全くなくなるので、安全性が高まる。

【００２０】請求項４によるファイアウォールは、認証データベース（パスワード記憶手段）またはパスワード取得手段１６から得たパスワードＶを平文のパスワードＷに戻したのちに、その平文のパスワードＷを使って電子メールサーバ２に対する電子メールの要求を行なう。すなわち、請求項４の発明によれば、認証データの一部として記憶しておくパスワードを暗号化しておける。そのため、請求項３の発明の効果に加えて、

【００２１】　認証データそのものを見るだけではパスワードが判らないので、認証データにアクセスする他のユーザや管理者からの秘匿の必要性がなくなり、認証データへのアクセスを細かく制限する手間を省ける。

【００２２】

【実施例】　まず、本発明によるファイアウォールを使用するときの、ネットワークの接続を図５に例示する。３０は本発明によるファイアウォールであり、通信チャンネル３６と通信チャンネル３７に接続されている。ルータ３４と３５は、通信チャンネルの経路を選択する装置である。ルータ３４を介してインターネット３９は通信チャンネル３６に接続され、ルータ３５を介して社内の別のネットワーク３８は通信チャンネル３７に接続されている。通信はルータを経由して行なうことができるので間接的にではあるが、ユーザ２９は通信チャンネル３６に接続され、電子メールサーバ３１は通信チャンネル３７に接続されていることになる。請求項２による発明の場合を図示するために、認証サーバ３２が、通信チャンネル３７に接続されている。請求項１による発明の場合は、ユーザ２９の認証はファイアウォール３０自身が行なうので、認証サーバをファイアウォールとは別に設ける必要はない。請求項１または２における使い捨てパスワードは、正規の認証に使用した後は使えなくなる性質のものである。例えば、一定期間だけ使用できるパスワードや１回だけ使用できるパスワード（ワンタイムパスワード）で実施すれば良い。以降では、ワンタイムパスワードの場合で説明する。図５において、ユーザ２９が電子メールサーバ３１から自己の電子メールを取り出すには、次のような手続きを経る。

【００２３】１、予め、ユーザ２９は自分のユーザ名と電子メールサーバ３１に対するパスワードＷを認証サーバ３２上のデータベースに登録しておく。この際、電子メールサーバ３１に対するパスワードは暗号化したパスワードＶを登録しておく。

【００２４】２、ユーザ２９はワンタイムパスワード発生装置３３を使って、ファイアウォール３０に認証させる。後の処理を簡潔に進めるため、この際、電子メールサーバ３１で必要となる情報も合わせてファイアウォールに伝えておくと良い。例えば、電子メールサーバ３１における電子メールアドレスと、ネットワーク上でのファイアウォール名を％で結合して、ｕｓｅｒ＠ｏｆｆｉｃｅ．ｃｏｍｐａｎｙ．ｃｏ．ｊｐ％ｆｗ．ｃｏｍｐａｎｙ．ｃｏ．ｊｐというフォーマットで送る。

【００２５】３、ファイアウォール３０は、ユーザ２９から受信したワンタイムパスワード等の情報を認証サーバ３２に送り、認証を求める。

【００２６】４、認証サーバは認証を行なう。認証が成

功したら（正規のユーザと認められたら）、認証サーバデータベースから暗号化されたパスワードＶを取出し、「認証が成功した」旨と、この暗号化パスワードＶをファイアウォール３０に回答する。

【００２７】５、ファイアウォール３０は、暗号化パスワードＶを平文のパスワードＷに復号し、ユーザのメールアドレス等と共に電子メールサーバ３１に送って、電子メールのやりとりを行なうセッションを開設する。

【００２８】６、以降は、ファイアウォール３０は、ユーザ２９からの電子メールの要求を通信チャンネル３６から出されたのと同じ形式に直して電子メールサーバ３１に伝え、電子メールサーバ３１からの回答をユーザ２９に伝える。

【００２９】なお、請求項１の発明は、認証サーバ３２にいちいち問い合せるのではなく、ファイアウォール３０の中で認証処理を行なうようにすれば実施できる。

本発明のファイアウォール３０は、各構成要素をハードウエアによって実施する他、計算機上で動作するソフトウエアによって実施することもできる。計算機としては、ファイアウォール専用の装置を使用する以外に、パソコンやワークステーション等の汎用の計算機を使用することもできる。パソコンやワークステーションを使用するときは、複数のプロセスを並行して動作させるオペレーティングシステム（例えば、ＵＮＩＸ）を採用し、そのオペレーティングシステムの中心部分（カーネル）と、その中心部分を補助するアプリケーションソフト（デーモンプロセス）に本発明に必要な機能をそれぞれ分担させて実施すると好適である。本発明を実施するためのデーモンプロセスを以降は、ＰＯＰ３ｐｒｏｘｙデーモンと呼ぶことにする。本発明をワークステーションで実施するときの、ワークステーション４０の構成を図６に示す。請求項２と３と４を、ワークステーションで動作するソフトウエアの処理フローを図７以降に示す。

【００３０】図６において、ＣＰＵ（マイクロプロセッサ）４１は、ＲＡＭ（ランダムアクセスできる読み書き可能なメモリ）４３に格納されたプログラムを、ＲＡＭ４３と磁気ディスク４２を作業領域として使用しながら実行する。６５はブートＲＯＭ（リードオンリーメモリ）である。ＣＰＵ４１は、電源立ち上げ時にブートＲＯＭ上のプログラムに従って、磁気ディスク４２に格納されたプログラムをＲＡＭ４３に転送し、以降はＲＡＭ４３上でプログラムを実行する。ＣＰＵ４１は、イーサネットインターフェイス４５を使って通信チャンネル４７と通信し、イーサネットインターフェイス４６を使って通信チャンネル４８と通信する。なお、キーボードとディスプレイは、ワークステーション４０がファイアウォールとして機能する際には本質的に不要なので、図から省いてある。

【００３１】図７は、イーサネットインターフェイス４５に通信が来たときにカーネルで実行すべき処理のフローを示している。この処理は、イーサネットインターフェイス４５がＣＰＵ４１に割り込みを掛けることによって起動される（Ｓ７０１）。Ｓ７０２は、イーサネットインターフェイス４５からイーサネットパケットを読み出す処理である。イーサネットパケットとして、各種のプロトコルのパケット、あるいは、電気的な雑音により欠損したパケットが読み出される。本実施例のファイアウォールでは、正規のＩＰパケットのみを通過させたいので、Ｓ７０３でＩＰパケットか否かを判別し、ＩＰパケットではないものをＳ７０４で廃棄している。Ｓ７０５は、ＩＰパケットに付随するプロトコル番号、ポート番号、ＩＰアドレス等のパケット情報を参照する処理である。ここで得たパケット情報を用いてＳ７０６以降の処理が行なわれる。Ｓ７０６では、処理対象となっているＩＰパケットを、通信チャンネル４８に通過させる、すなわち、フィルタリングするかを判断する。どのような種類のＩＰパケットをフィルタリングするかは、フィルタリング情報データベースＳ７０７に蓄えてある。フィルタリングしないＩＰパケットはＳ７０８で廃棄する。フィルタリングするＩＰパケットはＳ７０９で、自分宛て（ファイアウォール宛て）か否かを判断する。ファイアウォール宛てで無いならば、単に通信チャンネル４８に中継すれば良いパケットなので、Ｓ７１０で通信チャンネル４８に適合する形にＩＰパケットを構築し、Ｓ７１１で経路情報データベースＳ７１２を参照してＩＰパケットの送り先情報を追加して、Ｓ７１３でイーサネットインターフェイス４６へイーサネットパケットを書込む。

【００３２】一方、Ｓ７０９で、ファイアウォール宛てと判断されたならば、Ｓ７１４以降の処理に進む。単に通信チャンネル４８を通過させるのではなく、ファイアウォールで独自の処理が必要となるのは、本発明による電子メールだけでなく、ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、やＴＥＬＮＥＴ（Ｔｅｌｎｅｔ Ｐｒｏｔｏｃｏｌ）の場合もある。これらは、パケット情報の中の ポート番号によって区別できる。Ｓ７１４で、ＦＴＰに関するＩＰパケットと判断された場合は、Ｓ７１５でＦＴＰｐｒｏｘｙデーモンにそのパケットを渡す。Ｓ７１６で、ＴＥＬＮＥＴに関するＩＰパケットと判断された場合は、Ｓ７１７でＴＥＬＮＥＴｐｒｏｘｙデーモンにそのパケットを渡す。Ｓ７１８で、ＰＯＰ３に関するＩＰパケットと判断された場合は、Ｓ７１９でＰＯＰ３ｐｒｏｘｙデーモンにそのパケットを渡す。Ｓ７２０で、開設済みのセッションと判断された場合は、そのセッションを開設しているアプリケーションにそのパケットを渡す。アプリケーションには、たとえば、ＦＴＰｐｒｏｘｙデーモン、ＴＥＬＮＥＴｐｒｏｘｙデーモン、ＰＯＰ３ｐｒｏｘｙデーモンがある。これらのアプリケーションには、通常は、Ｓ７１５，Ｓ７１６，Ｓ７１７でそれぞれＩＰパケットを渡さ

れるが、認証サーバとの通信等を行なうためのセッションを開設した際はそのセッションに関するＩＰパケットはＳ７２１で渡される。Ｓ７２０で、開設済みセッションにも該当しない場合は、そのＩＰパケットに対応する処理が無いので、Ｓ７２２でそのパケットを廃棄する。Ｓ７２３は、カーネルの処理を終えた後のリターンを示している。すなわち、Ｓ７０１からの割り込みが処理の前の状態に復帰する。なお、Ｓ７１５，Ｓ７１７，Ｓ７１９，Ｓ７２１において、カーネルからＩＰパケットを各アプリケーションに渡すのは、オペレーティングシステムに用意されているプロセス間通信の機能を利用すれば良い。Ｓ７１５やＳ７１７によって実現されるＦＴＰやＴＥＬＮＥＴに関するファイアウォールの機能は公知技術なので説明を省く。

【００３３】図８は、図７のカーネルからのＩＰパケットを受け取るＰＯＰ３ｐｒｏｘｙデーモンの処理フローである。Ｓ８０１は、図７のＳ７１９又はＳ７２１からのＩＰパケットを受け取る処理である。このＩＰパケットは、ＰＯＰ３に関するものに限られるので、以降ではＰＯＰ３パケットと呼ぶことにする。電子メールサーバに対してログインを済ませて、電子メールに関する要求をだせる状態になっているかによって、以降の処理は異なる。Ｓ８０２は、そのＩＰパケットのユーザに関して、電子メールサーバへのログインが既に行なわれているかを判断する。もし、ログイン済みならば、ユーザから来たそのＰＯＰ３パケットを電子メールサーバに中継すれば良い。具体的には、Ｓ８０３で通信チャンネルＢに適合する形にＩＰパケットを構築し、Ｓ８０４でカーネルに対してそのＩＰパケットを送信する要求を行なう。送信要求とは、具体的には、カーネルをソフトウエアによる割り込みで起動し（図７のＳ７２４）、Ｓ７１１、Ｓ７１３の処理を行なわせる。その後は、Ｓ７２３でカーネルからリターンし、図８のＳ８０４の次に進む。

【００３４】Ｓ８０１で受け取ったＰＯＰ３パケットのユーザに関して電子メールサーバへのログインが済んでいないならば、Ｓ８０２の後はＳ８０５に進む。Ｓ８０５ではＰＯＰ３パケットの中身を見て、以降の認証及びログイン処理を行なうべきか判断する。すなわち、ワンタイムパスワードと「電子メールアドレス％ファイアウォール名」という内容になっているかを判断する。もし、これらの内容が揃っていなければ、認証ができないのでＳ８１９でそのＰＯＰ３パケットを廃棄する。一方、これらの内容が揃っていれば、認証及びログイン処理に進む。

【００３５】Ｓ８０６では、ＰＯＰ３パケットに含まれる電子メールアドレスのユーザ名とワンタイムパスワードを取出し、Ｓ８０８で認証サーバに送って、Ｓ８０９で認証結果を得る。認証サーバへの問い合せと回答受領のために、専用のセッションをＳ８０７で開設し、Ｓ８１０で閉じている。後述の図９のＳ９２０を経由して、カーネルはこの回答を、Ｓ８０９に渡している。認証サーバで行なわれる、ワンタイムパスワードを使った認証は、公知の技術を使うことができる。たとえば、文献Ｎｅｉｌ Ｈａｌｌｅｒ，“Ｔｈｅ Ｓ／ＫＥＹ Ｏｎｅ－Ｔｉｍｅ Ｐａｓｓｗｏｒｄ Ｓｙｓｔｅｍ”Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ ＩＳＯＣ ｓｙｍｐｏｓｉｕｍ ｏｎ Ｎｅｔｗｏｒｋ ａｎｄ Ｄｉｓｔｒｉｂｕｔｅｄ Ｓｙｓｔｅｍ Ｓｅｃｕｒｉｔｙ，Ｆｅｂｒｕａｒｙ １９９４，Ｓａｎ Ｄｉｅｇｏ，ＣＡや、Ｎｅｉｌ Ｈａｌｌｅｒ，Ｔｈｅ Ｓ／ＫＥＹ Ｏｎｅ－Ｔｉｍｅ Ｐａｓｓｗｏｒｄ Ｓｙｓｔｅｍ，ＲＦＣ１７６０，Ｂｅｌｌｃｏｒｅ，Ｆｅｂｒｕａｒｙ １９９５にその説明がある。

【００３６】Ｓ８１１では、認証サーバからの回答を判断し、もし、「認証成功」でないならば、正規なユーザからのものではないので、Ｓ８１２でそのパケットを廃棄する。一方、「認証成功」ならば、正規のユーザからかもしれない。そこで、Ｓ８１３では認証サーバが認証結果と共に回答した暗号化パスワードを復号化して平文のパスワードに直し、Ｓ８１４ではユーザ名と平文のパスワードを使用して電子メールサーバにログインする。なお、パスワードの暗号化と復号化は、公知の技術を使うことができる。たとえば、文献ＵＳ Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕｏｆ Ｓｔａｎｄａｒｄｓ，“Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ”，Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕ ｏｆ Ｓｔａｎｄａｒｄｓ，“Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ（ＦＩＰＳ）Ｐｕｂｌｉｃａｔｉｏｎ４６，Ｊａｎｕａｒｙ １９７７にその説明がある。

【００３７】電子メールサーバの状況により（たとえば、ログイン済みのユーザの数が、システムの限界に達しているとき）、ログインに失敗することがある。その場合は、Ｓ８１５からＳ８１６に進んで、そのパケットを廃棄する。一方、電子メールサーバへのログインが成功したときは、Ｓ８１７で、ログインに成功した旨を作業領域に記憶し、Ｓ８１８ではユーザに対してはプロンプト（次の入力を行なっても良いという旨のメッセージ）を送る。なお、請求項１の発明を実施するときは、認証に必要なデータベース７の内容を磁気ディスク４２に蓄えておき、そのデータベースを使って認証処理を行なうことをＳ８０６～Ｓ８１０の代わりに行なえば良い。

【００３８】図７と図８は、通信チャンネル４７からイーサネットパケットが送られてきたときの処理であるが、通信チャンネル４８からイーサネットパケットが送られてきたときのときも類似の処理となる。カーネルのすべき処理を、図８の処理フローとほぼ同じである。異

なる点は、通信の向きが逆なので、Ｓ９０１はイーサネットインターフェイス４６からの割り込みで起動され、Ｓ９０２ではイーサネットインターフェイス４６からイーサネットパケットを読み出すこと、Ｓ９１３ではイーサネットインターフェイス４５にイーサネットパケットを書き込むこと、Ｓ９１０やＳ９１１では通信チャンネル４７に適合する形でＩＰパケットの構築や送り先が決定されること、Ｓ９１９とＳ９２１でパケットを渡す相手が図１０に示すＰＯＰｐｒｏｘｙデーモンであること、である。

【００３９】図１０は、通信チャンネル４８から通信チャンネル４７に、電子メールに関するパケットを渡すためのＰＯＰｐｒｏｘｙデーモンのフローである。オペレーティングシステム上には、図８のＰＯＰｐｒｏｘｙデーモン、も、図１０のＰＯＰｐｒｏｘｙデーモン、も、共に存在している。開設済みのセッションに関するＰＯＰ３パケットを受け取って、中継する点は、同様の動作となるので、Ｓ８０１からＳ８０４までの処理と、Ｓ１００１からＳ１００４までの処理はほぼ同じである。ただし、Ｓ１００３では通信チャンネル４７に適合する形でＩＰパケットが構築され、Ｓ１００４は通信チャンネル４７に送信するため図９のＳ９２４以降の処理を呼び出す点が異なる。本実施例では、内部通信チャンネルにいるユーザが、外部通信チャンネルにある電子メールサーバを利用しない場合を例示しているので、Ｓ８０５からＳ８１８までに相当するユーザ認証やログイン処理をせずに、Ｓ１００５では単にパケットを廃棄している。なお、電子メールサーバの利用を終えるために、ユーザから電子メールサーバに終了を示すコマンドを送った後は、電子メールサーバからユーザに終了した旨のメッセージ（ログアウトの応答）が返される。Ｓ１００６でこのログアウトの応答を検出したときは、Ｓ１００７で、当該ユーザの電子メールサーバへのログインが成功した旨の記憶（Ｓ８１７で記憶した内容）を消去する。

【００４０】以上の説明から判るように、本発明を構成するユーザ認証問合手段１５は、Ｓ８０７からＳ８１０で実施されている。電子メール転送要求代理手段１３は、通信チャンネル４からのパケットがＳ７０２、Ｓ７１９、Ｓ８０１、Ｓ８０４、Ｓ７２４、Ｓ７１３を経て通信チャンネル４８に送信されることで実施されている。電子メール転送応答代理手段１４は、通信チャンネル４８からのパケットがＳ９０２、Ｓ９１９、Ｓ１００１、Ｓ１００４、Ｓ９１４、Ｓ９１３を経て通信チャンネル４７に送信されることで実施されている。パスワード取得手段１６は、Ｓ８０９で認証サーバからパスワードを受け取ることで実施されている。復号化手段１２は、Ｓ８１３で、暗号化パスワードを復号する処理で実施されている。ユーザ認証手段１１は、Ｓ８０７からＳ８１０における、認証サーバ８への問い合せの代わりに、認証処理を行なえば実施できる。その際、認証に必要なデータと共に、電子メールサーバへのパスワードを磁気ディスク４２に蓄えておけば、磁気ディスク４２がパスワード記憶手段の実施例となる。

【００４１】本発明のファイアウォールを図５から図１０に記載の具体例を用いて説明してきたが、本発明の実施はこの実施例に限られるものではない。上述の説明を参照すればこの実施例以外の代替例、変形例、変更例は当業者には容易に考えつくものと思われる。

【図面の簡単な説明】

【図１】本発明の構成を示す第１のブロック図

【図２】本発明の構成を示す第２のブロック図

【図３】イントラネットを用いた電子メールシステム概念図

【図４】イントラネットを外部通信チャネルへ接続した電子メールシステム概念図

【図５】本発明を実施したファイアウォールの実施例

【図６】本発明を実施したファイアウォールのハードウエア構成

【図７】本発明を実施したファイアウォールのカーネル処理のフローチャート（外部ユーザがファイアウォールに対して接続要求した場合）

【図８】本発明を実施したＰＯＰ３　ｐｒｏｘｙデーモンの電子メール転送要求処理のフローチャート（外部ユーザがファイアウォールに対して接続要求した場合）

【図９】本発明を実施したファイアウォールのカーネル処理のフローチャート（電子メールサーバがファイアウォールに対して接続要求した場合）

【図１０】本発明を実施したＰＯＰ３　ｐｒｏｘｙデーモンの電子メール転送要求処理のフローチャート（電子メールサーバがファイアウォールに対して接続要求した場合）

【符号の説明】

１：ファイアウォール
２：電子メールサーバ
３：ユーザ
４：通信ネットワーク
５：通信ネットワーク
７：認証データベース
８：認証サーバ
１１：ユーザ認証手段
１２：復号化手段
１３：電子メール転送要求代理手段
１４：電子メール転送応答代理手段
１５：ユーザ認証問合せ手段
１６：パスワード取得手段
２０：ファイアウォール
２１：電子メールサーバ
２２：イントラネット
２３：ユーザ用コンピュータ
２４：ユーザ用コンピュータ

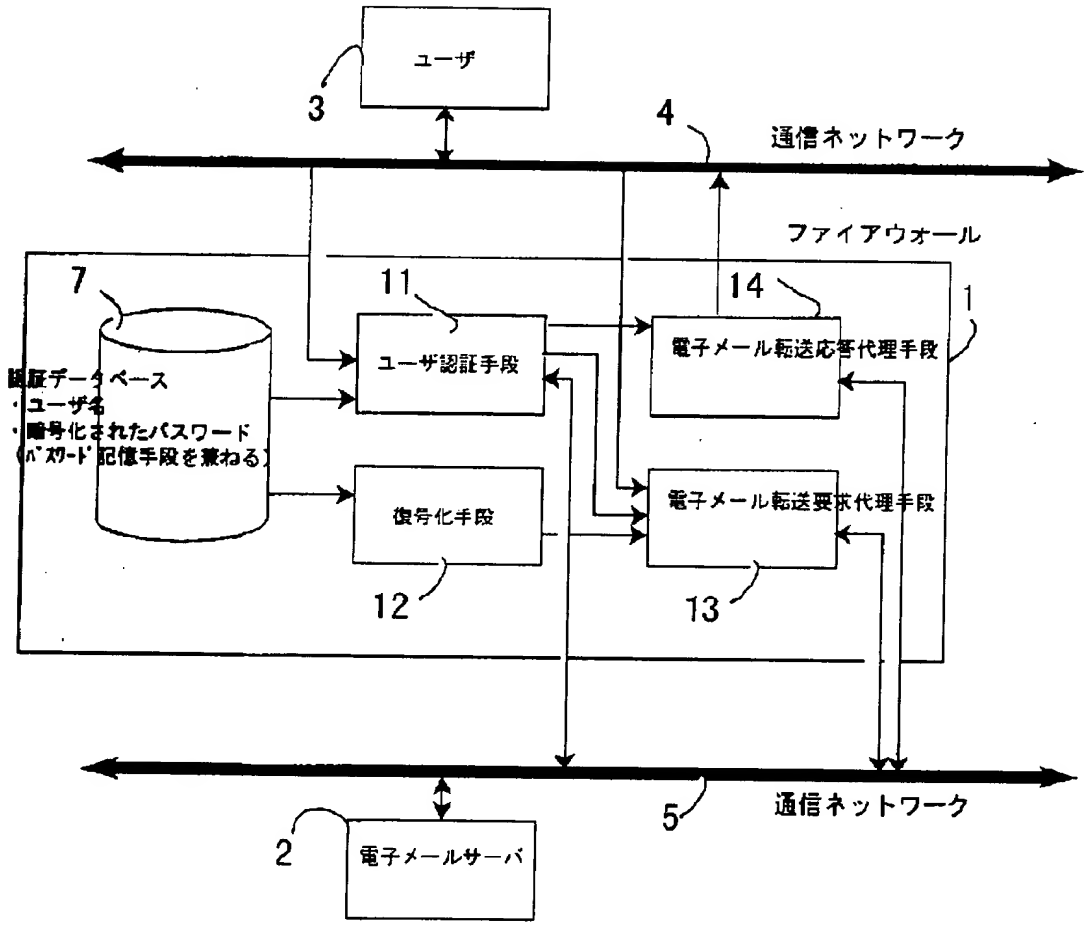
15

２５：ユーザ用コンピュータ
２６：ユーザ用コンピュータ
２７：外部ユーザ用コンピュータ
２８：外部通信チャンネル
２９：外部ユーザ
３０：ファイアウォール
３１：電子メールサーバ
３２：認証サーバ
３３：ワンタイムパスワード発生装置
３４：ルータ
３５：ルータ
３６：通信チャンネル

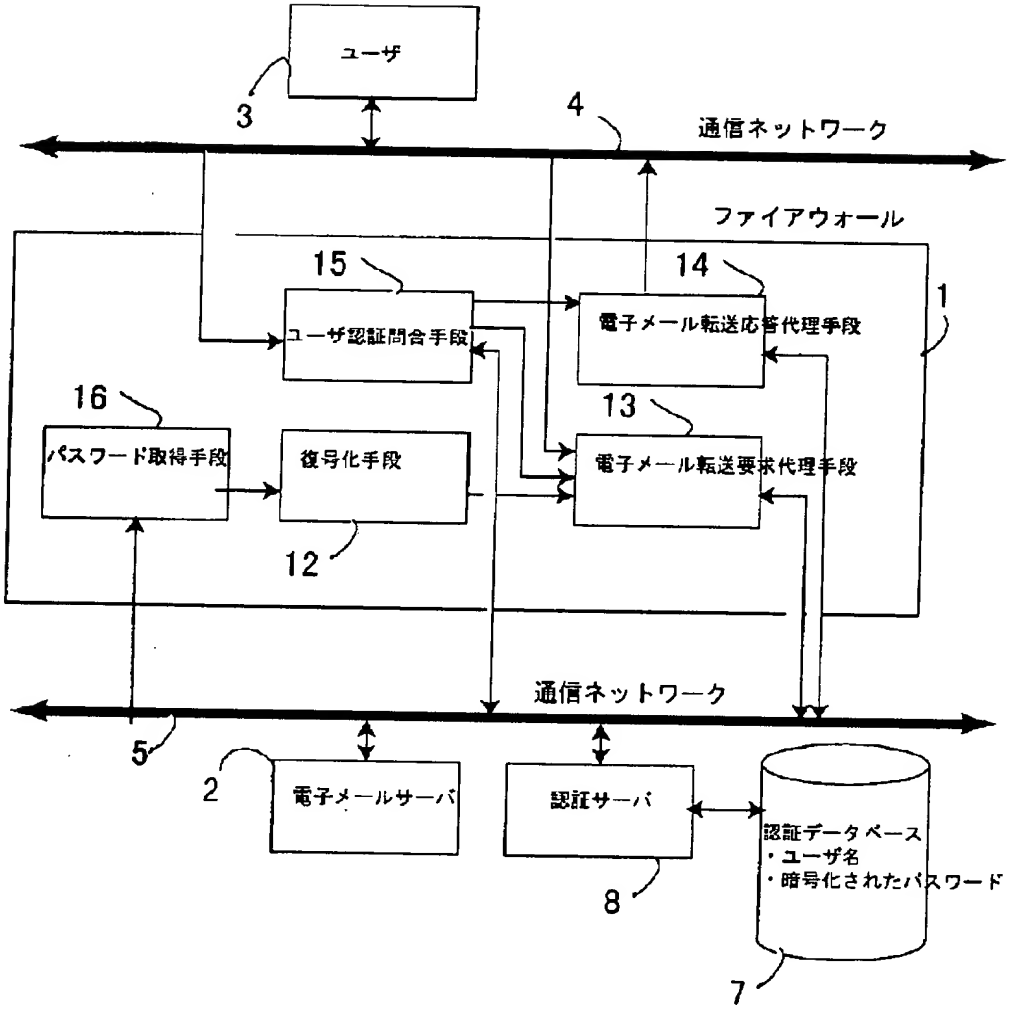
16

３７：通信チャンネル
３８：通信チャンネル
３９：インターネット
４０：ワークステーション
４１：ＣＰＵ（マイクロプロセッサ）
４２：磁気ディスク装置
４３：ランダムアクセスメモリ
４４：ブートＲＯＭ
４５：イーサネットインターフェイス
４６：イーサネットインターフェイス
４７　　通信チャネル
４８　　通信チャネル

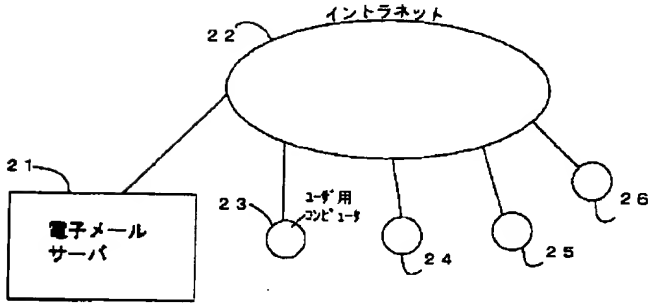
【図１】



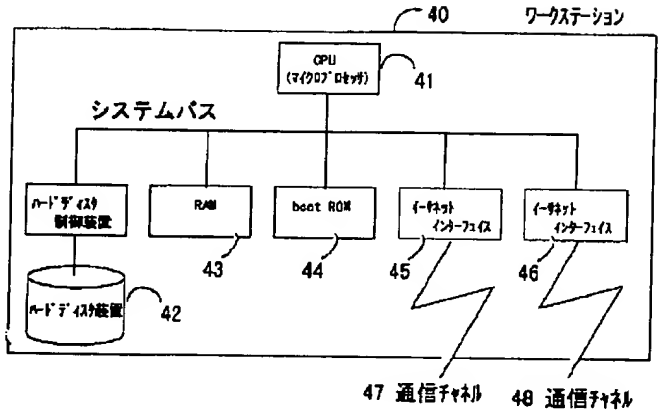
【図２】


ユーザ
3
4
通信ネットワーク
ファイアウォール
15
14
1
ユーザ認証問合手段
電子メール転送応答代理手段
16
13
パスワード取得手段
復号化手段
電子メール転送要求代理手段
12
通信ネットワーク
5
2
電子メールサーバ
認証サーバ
認証データベース
・ユーザ名
・暗号化されたパスワード
8
7

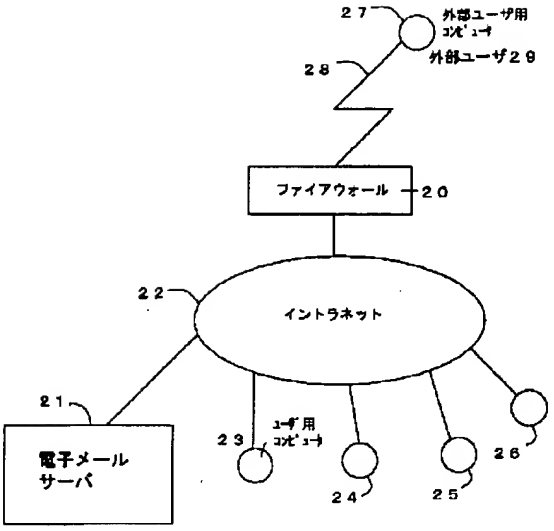
【図３】


イントラネット
22
21
電子メール
サーバ
23
ユーザ用
コンピュータ
24
25
26

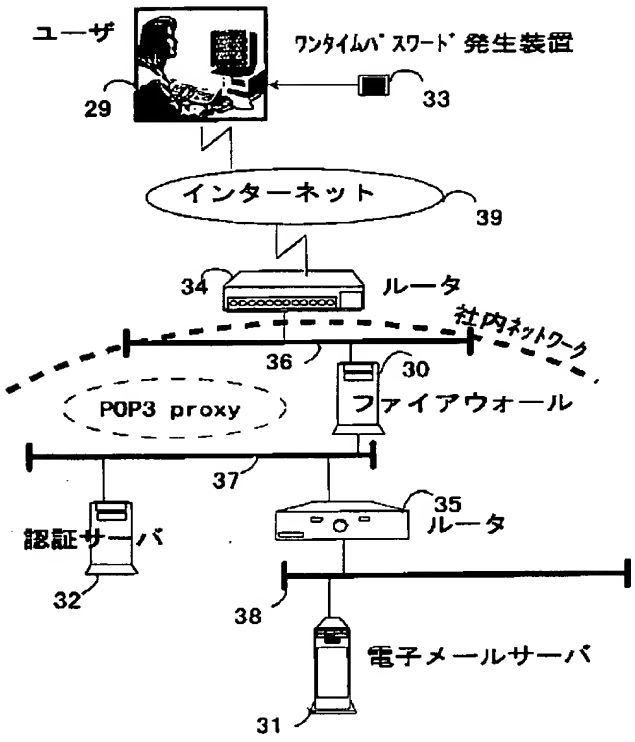
【図６】


40
ワークステーション
CPU
(マイクロプロセッサ)
41
システムバス
ハードディスク
制御装置
RAM
boot ROM
イーサネット
インターフェイス
イーサネット
インターフェイス
43
44
45
46
ハードディスク装置
42
47 通信チャネル
48 通信チャネル

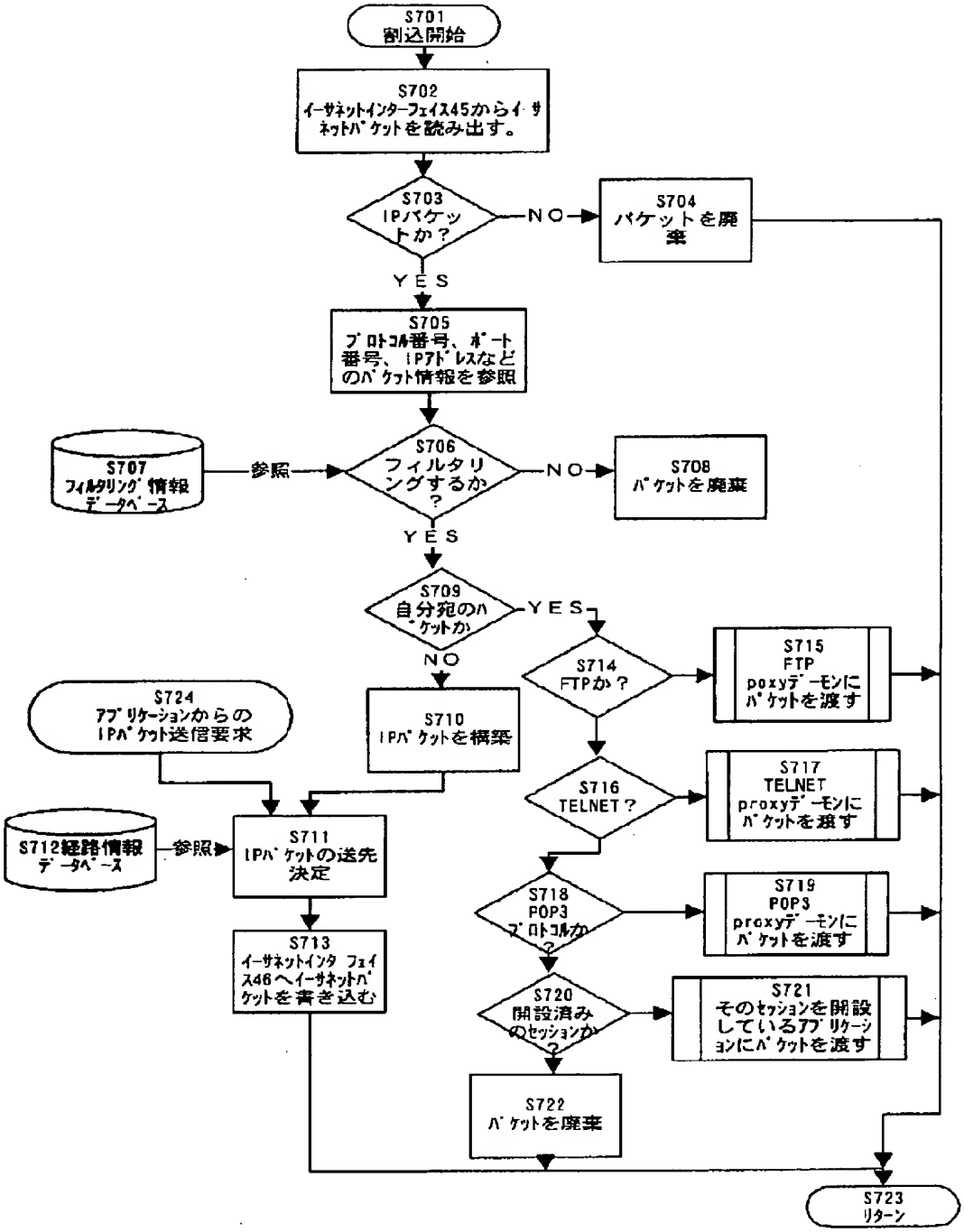
【図４】


27
外部ユーザ用
ｺﾝﾋﾟｭｰﾀ
外部ユーザ29
28
ファイアウォール
20
22
イントラネット
21
電子メール
サーバ
23
ﾕｰｻﾞ用
ｺﾝﾋﾟｭｰﾀ
24
25
26

【図５】


ユーザ
ワンタイムパスワード発生装置
29
33
インターネット
39
34
ルータ
社内ネットワーク
36
30
POP3 proxy
ファイアウォール
37
35
ルータ
認証サーバ
32
38
電子メールサーバ
31

【図７】


S701
割込開始
S702
イーサネットインターフェイス45からイーサネットパケットを読み出す。
S703
IPパケットか？
NO
S704
パケットを廃棄
YES
S705
プロトコル番号、ポート番号、IPアドレスなどのパケット情報を参照
S707
フィルタリング情報データベース
参照
S706
フィルタリングするか？
NO
S708
パケットを廃棄
YES
S709
自分宛のパケットか
YES
NO
S714
FTPか？
S715
FTP proxyデーモンにパケットを渡す
S716
TELNET？
S717
TELNET proxyデーモンにパケットを渡す
S718
POP3プロトコルか？
S719
POP3 proxyデーモンにパケットを渡す
S720
開設済みのセッションか？
S721
そのセッションを開設しているアプリケーションにパケットを渡す
S722
パケットを廃棄
S724
アプリケーションからのIPパケット送信要求
S710
IPパケットを構築
S712経路情報データベース
参照
S711
IPパケットの送先決定
S713
イーサネットインタフェイス46へイーサネットパケットを書き込む
S723
リターン

【図８】

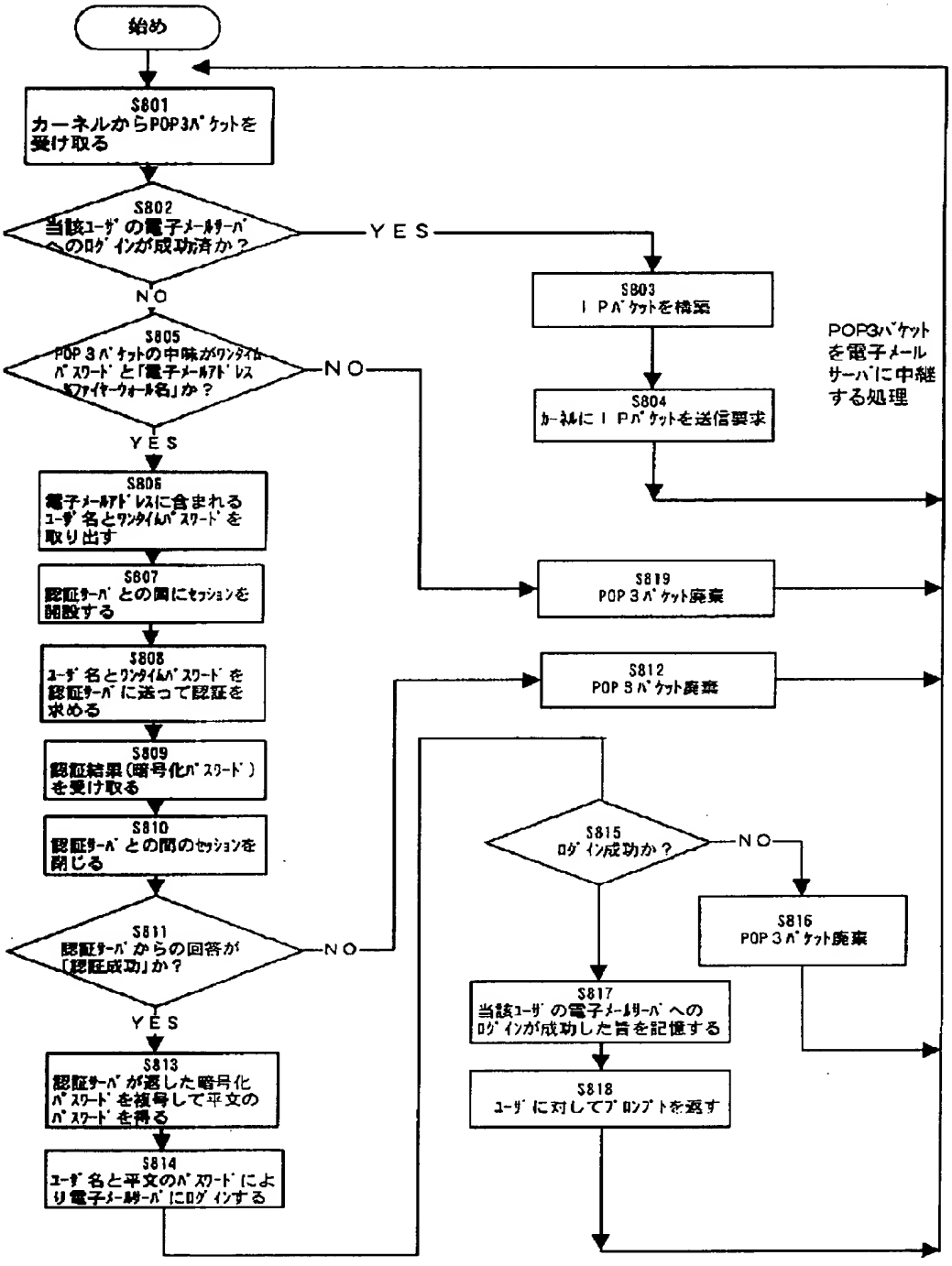


図８　POP3 proxyﾃﾞｰﾓﾝ 電子ﾒｰﾙ転送(外部通信ﾁｬﾝﾈﾙ → 内部通信ﾁｬﾝﾈﾙ)要求処理ﾌﾛｰ
(外部ﾕｰｻﾞからﾌｧｲｱｳｫｰﾙに対して要求したときの処理)

【図９】

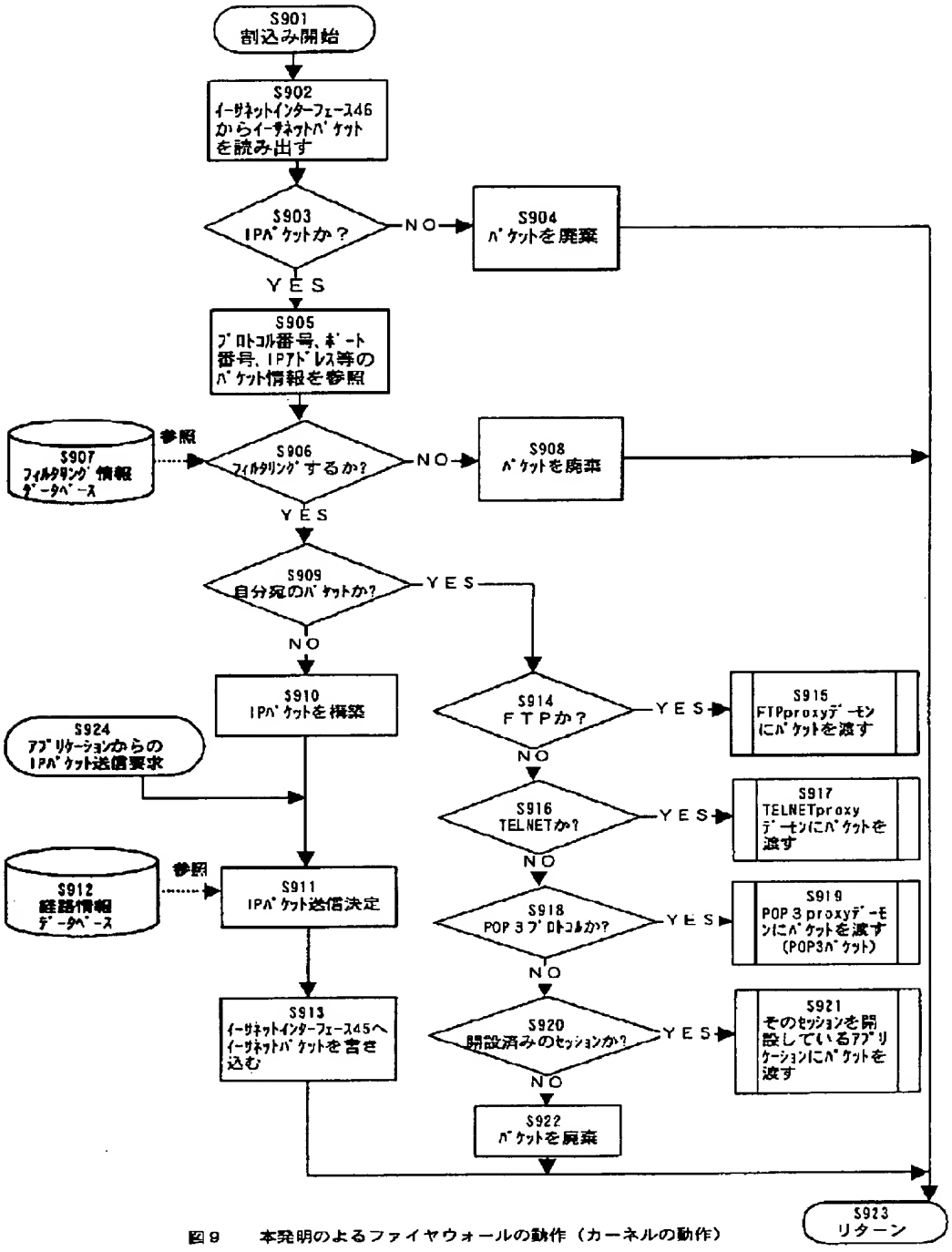
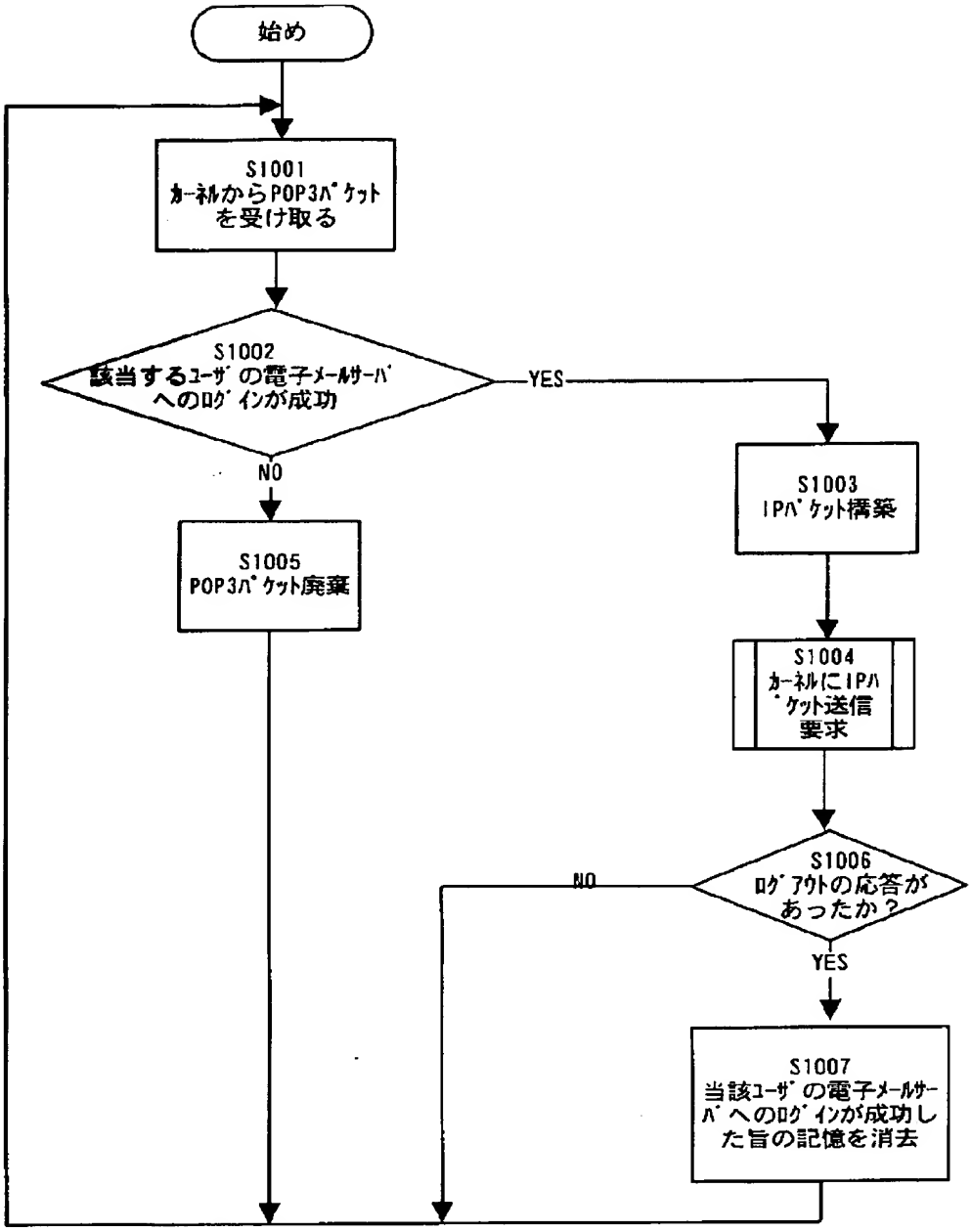


図９　本発明のよるファイヤウォールの動作（カーネルの動作）

【図１０】


始め
S1001
ｶｰﾈﾙからPOP3ﾊﾟｹｯﾄを受け取る
S1002
該当するﾕｰｻﾞの電子ﾒｰﾙｻｰﾊﾞへのﾛｸﾞｲﾝが成功
YES
NO
S1003
IPﾊﾟｹｯﾄ構築
S1004
ｶｰﾈﾙにIPﾊﾟｹｯﾄ送信要求
S1005
POP3ﾊﾟｹｯﾄ廃棄
S1006
ﾛｸﾞｱｳﾄの応答があったか？
NO
YES
S1007
当該ﾕｰｻﾞの電子ﾒｰﾙｻｰﾊﾞへのﾛｸﾞｲﾝが成功した旨の記憶を消去